REMARKS

Claim 1-2, 4-8, 10-14 and 16-18 were examined by the Office, and in the final Office Action of January 27, 2009 all claims are rejected. In the Notice of Panel Decision of July 7, 2009 the Office maintained the rejections of the final Office Action of January 27, 2009. With this response, claims 1, 7 and 13 are amended. All amendments are fully supported by the specification as originally filed. Support for the amendments can be found at least from page 11, lines 28-33 of the specification. Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

This response is submitted along with a Request for Continued Examination (RCE).

Claim Rejections Under § 103

On page 3 of the Office Action, claims 1-2, 4-8, 10-14 and 16-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan (U.S Patent No. 6,968,459) in view of Grawrock (U.S. Appl. Publ. No. 2003/0196100). Applicant respectfully submits that claim 1 is not disclosed or suggested by the cited references, alone or in combination, because the cited references fail to disclose or suggest all of the limitations recited in claim 1. Claim 1 is amended to clarify that the storage area in the storage circuit has protected data relating to security functions of the circuitry and protected applications. The amendments to claim 1 clarify that the protected data is the same protected data, since it relates to the security functions of the circuitry. This is in contrast to the information loaded or accessed from a removable storage device as in Morgan. Furthermore, the cited references at least fail to disclose or suggest storage circuit access control means arranged to enable the processor to access the storage area in which the protected data are located when a first processor operating mode is set, and storage circuit access control means arranged to prevent the processor from accessing the storage area in which protected data are located when a second processor operating mode is set, as recited in claim 1.

In contrast to claim 1, Morgan is directed to a secure computing environment in which a computer automatically operates in a secure full access data storage mode when the computer detects the presence of a secure removable storage device, and automatically operates in a restricted-access mode if the computer senses a non-secure removable storage device. See Morgan column 1, lines 35-42. In Morgan, one or more removable media drives (121) are used to access one or more removable storage devices (151), and each storage device has a storage medium for holding digital information. See Morgan column 3, lines 5-10. In order to automatically detect whether a storage device (151) is a secure device, computer (100) determines whether device-specific security information was written to storage device (151). See Morgan column 4, lines 6-9. The computer (100) is configured to operate in a restricted-access mode upon power-up until removable storage device (151) is verified as secure, and a secure computing environment is provided when the user tries to boot directly from one of the removable storage devices (151). See Morgan column 7, lines 17-24. However, the storage devices (151) do not contain protected data that relates to the security functions of the circuitry, as recited in claim 1. This is because the storage devices (151) contain a variety of digital information that is dependent upon the storage device, i.e. whether it is a secure storage device or a non-secure storage device. Accordingly, claim 1 is amended to clarify that the storage area of claim 1 contains the same protected data, and access to the storage area is dependent upon which operating mode the processor is set in. Therefore, for at least this reason, claim 1 is not disclosed or suggested by the cited references.

In addition, applicant respectfully submits that Morgan does not disclose or suggest storage circuit access control means arranged to enable the processor to access the storage area in which protected data is located when a first processor operating mode is set. As recited in claim 1, the protected data relates to circuitry security, and when the first processor operating mode is set only authenticated software and protected applications have access to the protected data. However, in Morgan in step 204 the storage manager detects whether the storage device (151) is secure by attempting to read any device-specific security information from the storage device (151). See Morgan column 5, lines 7-10. In step 210 the storage manager retrieves manufacturing-specific security information, this security information may then be used in step 212 to generate a unique encryption key, but if it was not possible to retrieve the security information step 216 is performed in which the computer (100) is operated in a restricted-access data storage mode. See Morgan column 5, lines 47-63. In contrast to claim 1, the full-access mode or restricted-access mode is set based on the security information, i.e. protected data related to circuitry security. Access to the protected data is available before the full-access or restricted-access mode is set, and not after a first processor operating mode, i.e. secure mode, is set, as recited in claim 1. Therefore, for at least this reason claim 1 is not disclosed or suggested by the cited references.

Furthermore, Morgan also fails to disclose or suggest storage circuit access control means arranged to prevent the processor from accessing the storage area in which protected data is located when a second processor operating mode is set, thereby enabling the processor to execute non-verified software downloaded into the circuitry, as recited in claim 1. In contrast to claim 1, in Morgan the restricted-access mode is set when the security information is not retrievable from the storage circuitry. Therefore, in Morgan the second operating mode, i.e. restricted-access mode, is not set to prevent the processor from accessing the protected data. Instead, the second operating mode for the processor is set because the protected data is not retrievable from the storage circuitry. Therefore, Morgan also fails to disclose or suggest this limitation recited in claim 1.

Grawrock is directed to a method and device for protecting system secrets from system reset attacks. This is performed by locking the memory which contains the system secrets after a system reset, and by removing the secrets from the memory before the memory is unlocked. Grawrock fails to make up for the deficiencies in the teachings of Morgan identified above, and therefore the cited references, alone or in combination, fail to disclose or suggest all of the limitations recited in claim 1.

Therefore, for at least the reasons discussed above, claim 1 is not disclosed or suggested by the cited references. Independent claims 7 and 13 include limitations similar to those recited in claim 1. Therefore, independent claims 7 and 13 are not disclosed or suggested by the cited references for at least the reasons discussed above with respect to claim 1.

The claims rejected above, and depending from the above mentioned independent claims are not disclosed or suggested by the cited references at least in view of their dependencies. Furthermore, with respect to claims 4, 10 and 16, Morgan does not disclose or suggest means to indicate which mode the processor is operating. Instead, Morgan only states that the status manager repeats blocks 204 through 216 when a status change is detected for storage device (151), for example when the storage device (151) is removed from the removable media drive (121), and a new storage device is inserted. See Morgan column 6, lines 23-28. However, this does not indicate which mode the processor is operating, as recited in claims 4, 10 and 16. Therefore, for at least this additional reason, claims 4, 10 and 16 are not disclosed or suggested by the cited references.

On page 4 of the Office Action, claims 2, 6, 8, 12, 14 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Grawrock, and further in view of Sato (U.S. Appl. Publ. No. 2001/0055980), and on page 5 of the Office Action, claims 5, 11, and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Grawrock, and further in view of Ishidera (US Patent 2002/0040442 A1).

Sato is directed to a multi-mode cellular phone terminal supporting a plurality of communication systems, which multi-mode cellular phone terminal comprises a system timer for switching over a plurality of clocks and counting different timings to support a plurality of communications system. Ishidera is directed to a software apparatus which executes processes of software with reduced power consumption at the time of operation on a battery and a recording medium. The apparatus determines whether power saving is needed or not.

The cited references fail to make up for the deficiencies in the teachings of Morgan identified above, and because all of the rejected claims ultimately depend from an independent claim, the claims are not disclosed or suggested by the cited references.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and such action is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge Deposit Account No. 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,

Date: 20 August 2009

Keith R. Obert
Attorney for the Applicant
Registration No. 58,051

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
Telephone:(203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955